UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,814	03/14/2005	Jarmo Talvitie	3502-1075	4622

466 7590 05/22/2008

YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,814	TALVITIE, JARMO	
	Examiner	Art Unit	
	JEREMIAH AVERY	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-10,12,14-23,26,29-31,33,34,37 and 39-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-10,12,14-23,26,29-31,33,34,37 and 39-41* is/are rejected.

7)☒ Claim(s) *31* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 7, 11, 13, 24, 25, 27, 28, 32, 35, 36 and 38 have been cancelled.

2. Claims 1-6, 8-10, 12, 14-23, 26, 29-31, 33, 34, 37 and 39-41 have been examined.

3. Responses to Applicant's remarks have been given.

Claim Objections

1. Claim 31 is objected to because of the following informalities: grammatical error. The claim language, "having one more characteristics unknown to the apparatus..." is improper. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2, 3, 5, 14-21, 34 and 39 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

2. The above mentioned claims possess the claim language "adapted". It has been held that the recitation that an element is "adapted to" perform a function is not a positive limitation but only requires the ability to so perform. It does not constitute a limitation in any patentable sense. Please refer to In re Hutchison, 69 USPQ 138 for further clarification. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-6, 8-10, 12, 14-23, 26, 29-31, 33, 34, 37 and 39-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication No. US 2002/0116639 to Chefalas et al., hereinafter Chefalas and further in view of United States Patent Application Publication No. 2004/0030913 to Liang et al., hereinafter Liang.

3. Chefalas significantly discloses the claimed invention, as cited below but does not significantly disclose the claim limitations pertaining to "unknown malicious softwares having one or more characteristics unknown to said first sub-system" as found within independent claims 1, 22, 23, 31 and 39. However, Liang discloses these claim limitations, as cited below.

4. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Liang within the method and apparatus of Chefalas so that "the network system can, at the minimum, defend itself against damage from mail-borne viruses currently unknown to the virus database therein. Moreover, further analysis of the results of the profiling serves as the basis for developing antivirus countermeasures against the unknown viruses" (*Liang* – page 1, paragraph 10).

5. Regarding claim 1, Chefalas and Liang disclose a security system for repelling malicious softwares in computers and computer networks and that is configured to forward messages, the security system comprising a first sub-system to detect unknown malicious softwares having one or more characteristics unknown to said first sub-system, said first sub-system being configured in connection with the forwarding of messages or with other action or, in a timed manner, to perform at least a partial simulation to activate unknown malicious softwares having one or more characteristics unknown to said first sub-system and to detect the activated unknown malicious softwares by detecting consequences of activation of the unknown malicious softwares (*Chefalas* – page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraphs 30 and 32, page 4, paragraph 46 and page 5, paragraph 54 and *Liang* – page 1, paragraph 14, "determining if any of the trapped e-mails are infected by an unknown computer virus other than the known computer viruses stored in the virus

database", page 3, paragraphs 32, 35, 40, page 4, paragraphs 50 and 52-54 and page 5, remainder of paragraph 54 and paragraphs 56 and 58).

6. Regarding claim 2, Chefalas discloses the security system in accordance with claim 1, that is adapted to forward an alarm caused by the detection of the malicious softwares to at least one system connected to the security system (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraphs 30 and 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108" and page 4, paragraph 46).

7. Regarding claim 3, Chefalas discloses the security system in accordance with claim 1, that is further adapted to break a connection to at least one other system on the basis of an alarm caused by the detection of the malicious softwares (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraph 30 and page 4, paragraph 46).

8. Regarding claim 4, Chefalas discloses a second sub-system for forwarding messages from the first sub-system to at least one system connected to the security system (page 3, paragraph 32, "If the same type of virus occurs several times in a

specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

9. Regarding claim 5, Chefalas discloses a third sub-system that is adapted to break a connection to at least one other sub-system upon receiving an alarm (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraph 30, page 4, paragraph 46 and page 5, paragraph 54).

10. Regarding claim 6, Chefalas discloses wherein the at least one other sub-system includes an identifier which corresponds to an identifier of the third sub-system (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).

11. Regarding claim 8, Chefalas discloses wherein the alarm is a message or at least a part of a message that is forwarded to the recipient prior to other communications (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server" and page 3, remainder of paragraph 28).

12. Regarding claim 9, Chefalas discloses wherein the third sub-system includes at least one computer or one network element including a computer (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

13. Regarding claim 10, Chefalas discloses wherein the alarm is forwarded via a separate connection (page 1, paragraph 12 and page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

14. Regarding claim 12, Chefalas discloses wherein the consequences of activation of the malicious softwares detected by the first sub-system include at least one of: a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect the malicious softwares, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

15. Regarding claim 14, 28 and 36, Chefalas discloses wherein the first sub-system is adapted to choose one or more of the following logics when trying to activate the malicious softwares:

one defined by the user, pre-programmed or at least partially random logic (page 5, paragraph 60).

16. Regarding claim 15, Chefalas discloses further comprising a parallel system that is adapted to save a message sent from the third sub-system, the parallel system being connected in parallel with the third sub-system (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

17. Regarding claim 16, Chefalas discloses wherein the first sub-system is adapted to compare in the parallel system a message sent from the third sub-system to the first sub-system and additionally saved in the parallel system in order to detect an anomaly caused by a malicious software (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

18. Regarding claim 17, Chefalas discloses wherein the parallel system is adapted to forward a message saved by it (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

19. Regarding claim 18, Chefalas discloses the security system in accordance with claim 1, that is adapted to examine messages forwarded through the security system in order to detect known malicious softwares (page 1, paragraph 12, page 3, paragraph 30 and page 5, paragraph 54).

20. Regarding claim 19, Chefalas discloses the security system in accordance with claim 4, comprising first and second ones of the at least one system, wherein the security system is adapted to transfer data between the first and the second ones of the at least one system through the first and the second syb-systems, and wherein the security system is adapted to disrupt the connection between the first one of the at least one system and the first sub-system before a connection is established between the first and the second sub-systems and to disrupt the connection between the first and the second sub-systems before a connection is established between the second sub-system and the second one of the at least one system (page 1, paragraph 12, page 3, paragraph 30, "shut down the local server and/or the LAN" and page 5, paragraph 54).

21. Regarding claim 20, Chefalas discloses wherein said first sub-system is adapted to compare messages with at least partially identical identifiers with each other in order to detect unknown malicious softwares (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).

22. Regarding claim 21, Chefalas discloses wherein the first sub-system is adapted to request the sender of the messages with at least partially identical identifiers to re-send at least one of the messages and is further adapted to compare at least one re-sent message received with the original messages in order to detect messages containing malicious softwares (page 4, paragraphs 44, 45 and 47 and page 5, paragraph 58).

23. Regarding claim 22, Chefalas and Liang teach a method for repelling malicious softwares in computers and data networks, the method being carried out in a security system including a first sub-system for forwarding messages and for detecting malicious softwares having one or more characteristics unknown to said first sub-system and that is isolatable from the remainder of the security system (*Chefalas* – page 1, paragraph 12, page 2, paragraph 28 and page 3, remainder of paragraph 28 and paragraph 30, "shut down the local server and/or the LAN" and *Liang* – page 1, paragraph 14, "determining if any of the trapped e-mails are infected by an unknown computer virus other than the known computer viruses stored in the virus database", page 3, paragraphs 32, 35, 40, page 4, paragraphs 50 and 52-54 and page 5, remainder of paragraph 54 and paragraphs 56 and 58), the method includes the steps where:

functions of the security system are monitored by the first sub-system in order to detect consequences of activation, in an at least partial simulation, of an unknown malicious software having one or more characteristics unknown to said first sub–system (Chefalas – page 1, paragraph 12, page 2, paragraph 28 and page 3, remainder of paragraph 28 and paragraph 30 and *Liang* – page 1, paragraph 14, "determining if any of the trapped e-mails are infected by an unknown computer virus other than the known computer viruses stored in the virus database", page 3, paragraphs 32, 35, 40, page 4, paragraphs 50 and 52-54 and page 5, remainder of paragraph 54 and paragraphs 56 and 58), the consequences of activation including at least one of the following:
a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious softwares, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there,
a malicious software is detected when one of the consequences is detected, and an alarm is given (*Chefalas* – page 2, paragraph 28 and page 3, remainder of paragraph 28 and paragraph 30).

24. Regarding claim 23, Chefalas and Liang teach a method for repelling malicious softwares in computers and computer networks, the method comprising the steps of:

performing at least partial simulation to activate unknown malicious softwares having one or more characteristics unknown to an entity performing the method in connection with the forwarding of messages or other action, or in a timed manner, detecting the activated unknown malicious softwares by detecting consequences of activation of the malicious softwares caused by the at least partial simulation, and giving an alarm when a malicious software is detected (*Chefalas* – page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28 and page 3, remainder of paragraph 28 and paragraphs 29 and 30 and *Liang* – page 1, paragraph 14, "determining if any of the trapped e-mails are infected by an unknown computer virus other than the known computer viruses stored in the virus database", page 3, paragraphs 32, 35, 40, page 4, paragraphs 50 and 52-54 and page 5, remainder of paragraph 54 and paragraphs 56 and 58).

25. Regarding 26, Chefalas teaches wherein the method is run in a security system including a first sub-system and a second sub-system and wherein the consequences of activation of the malicious software include at least one of:

a change takes place in the first sub-system prior to actions causing changes carried out by the first sub-system, a change takes place in the first sub-system that is not an action taken by the first sub-system to detect a malicious software, a message leaves for another system without command from the first sub-system, a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraphs 25

and 28, page 3, remainder of paragraph 28 and paragraphs 30-32, page 4, paragraphs 44, 46 and 47 and page 5, paragraph 54).

26. Regarding claim 29, Chefalas teaches further comprising the step where known malicious softwares are searched for on the basis of their characteristics (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

27. Regarding claim 30, Chefalas teaches wherein the security system is connected to a first system and a second system and wherein data are transferred between the first system and the second system through the first sub-system and the second sub-system phase by phase in order (page 1, paragraph 12 and page 5, paragraph 54), in which phases:

the connection for data transfer is disrupted between the first system and the first sub-system, a connection for data transfer is established between the first sub-system and the second sub-system, the connection for data transfer is disrupted between the first sub-system and the second sub-system, a connection for data transfer is established between the second sub-system and the second system (page 5, paragraph 54).

28. Regarding claim 31, Chefalas and Liang disclose an apparatus for repelling malicious softwares in computers and computer networks, comprising equipment for saving data and for handling data and equipment for transferring data with another apparatus, wherein the apparatus is configured to receive a message and to perform an at least partial simulation to activate unknown malicious softwares having one more

characteristics unknown to the apparatus and contained in the message and to detect the activated unknown malicious softwares by detecting consequences of activation of the malicious softwares (*Chefalas* – page 2, paragraph 28 and page 3, remainder of paragraph 28 and paragraph 30 and *Liang* – page 1, paragraph 14, "determining if any of the trapped e-mails are infected by an unknown computer virus other than the known computer viruses stored in the virus database", page 3, paragraphs 32, 35, 40, page 4, paragraphs 50 and 52-54 and page 5, remainder of paragraph 54 and paragraphs 56 and 58).

29. Regarding claim 33, Chefalas discloses wherein the consequences of activation of the malicious software include at least one of: a change takes place prior to actions caused by changes made by the apparatus, a change takes place that is not an action taken by the apparatus to detect a malicious software (page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraphs 23 and 27).

30. Regarding claim 34, Chefalas discloses wherein the apparatus is adapted to send a message to either a sub-assembly of the apparatus or to said another apparatus (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108"), and wherein the consequences of activation of the malicious software include at least one of:

a message leaves without authorization from the anti-malicious software of the apparatus, a message leaves for an address it has not originally been directed to, a message does not leave although it has been given a command to be sent (page 2,

paragraphs 25 and 28, page 3, remainder of paragraph 28 and paragraphs 30-32 and page 4, paragraphs 44, 46 and 47).

31. Regarding claim 37, Chefalas discloses wherein the apparatus examines the message in order to detect known malicious softwares (page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

32. Regarding claim 39, Chefalas and Liang disclose a security system for repelling malicious software in a computer and that is adapted to forward messages, the security system comprising:

a first sub-system that detects unknown malicious software having one or more characteristics unknown to said first sub-system, said first sub-system being configured, in connection with forwarding of messages or with another action in a timed manner, to activate in an at least partial simulation an unknown malicious software having one or more characteristics unknown to said first sub-system and to detect the activated unknown malicious software by detecting a consequence of the activation of the malicious software (*Chefalas* – page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "VSC 126 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraphs 30 and 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108" and page 4, paragraph 46 and *Liang* – page 1, paragraph 14, "determining if any of the trapped e-mails are infected by an unknown computer

virus other than the known computer viruses stored in the virus database", page 3, paragraphs 32, 35, 40, page 4, paragraphs 50 and 52-54 and page 5, remainder of paragraph 54 and paragraphs 56 and 58);

an analyzing sub-system that receives files contaminated with an unknown malicious software from said first sub-system and that analyzes the unknown malicious software to provide fingerprints of the unknown malicious software and that forwards the fingerprints (*Chefalas* – page 1, paragraph 12, page 2, remainder of paragraph 12 and paragraph 28, "If the detected virus is the type of virus that can be replicated or cloned, VSC 128 at server 106 immediately severs the connection with client 112 and all other clients connected to the server", page 3, remainder of paragraph 28 and paragraphs 29, "benign viruses", 30 and 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108" and page 4, paragraphs 44 and 46 and *Liang* – page 1, paragraph 14, "determining if any of the trapped e-mails are infected by an unknown computer virus other than the known computer viruses stored in the virus database", page 3, paragraphs 32, 35, 40, page 4, paragraphs 50 and 52-54 and page 5, remainder of paragraph 54 and paragraphs 56 and 58).

33. Regarding claim 40, Chefalas discloses wherein the security system communicates with the computer network being protected by the security system, but is separate from the computer network (page 1, paragraph 12 and page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108").

34. Regarding claim 41, Chefalas discloses wherein the security system is in a gateway for the computer network (page 1, paragraph 12, page 3, paragraph 32, "If the same type of virus occurs several times in a specified time interval, server 106 sends a priority business event to the remote network administrator at server 108" and page 5, paragraph 59, "firewalls, servers or monitoring devices").

Response to Arguments

35. Pertaining to claims 39-41, the claim language "fingerprints", within the context as defined by the Applicant within the Specification, is broadly interpreted by the Examiner to pertain to characteristics/attributes of the claimed "malicious software".

36. Applicant's arguments, see page 12, filed 02/14/08, with respect to the objection to claim 22 have been fully considered and are persuasive. The objection of claim 12 has been withdrawn.

37. Applicant's arguments, see page 12, filed 02/14/08, with respect to the 35 U.S.C. 112, 2nd paragraph rejection of claims 1 and 31 have been fully considered and are persuasive. The 35 U.S.C. 112, 2nd paragraph rejection of claims 1 and 31 has been withdrawn. However, the 35 U.S.C. 112, 2nd paragraph rejection of claims 2, 3, 5, 14-21, 34 and 39 is maintained due to the claim language, "adapted to".

38. Applicant's arguments with respect to claims 1-6, 8-10, 12, 14-23, 26, 29-31, 33, 34, 37 and 39-41 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

39. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

40. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

41. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

42. The following United States Patents and Patent Application Publication are cited to further show the state of the art with respect to virus detection and removal, such as:

United States Patent No. 7,137,034 to Largman et al., which is cited to show a self repairing computer having user accessible switch for modifying bootable storage device configuration to initiate repair.

United States Patent No. 6,873,988 to Hermann et al., which is cited to show system and methods providing anti-virus cooperative enforcement.

United States Patent No. 7,089,589 to Chefalas et al., which is cited to show a method and apparatus for the detection, notification and elimination of certain computer viruses.

United States Patent No. 7,171,690 to Kouznetsov et al., which is cited to show a wireless malware scanning back-end system and method.

United States Patent No. 7,096,381 and United States Patent Application Publication No. US 2002/0194534 to Largman et al., which are cited to show on-the-fly repair of a computer.

43. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

44. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

45. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131